Remarks

Applicant respectfully requests review of this application. Claims 1-28 are currently pending. Claim 1, 2, 6-8, 11-13, 16, 21-23, and 26 are amended. No claims have been cancelled or added.

Thus, claims 1-28 are hereby presented for examination.

Claim Rejection under 35 U.S.C. §103

Devanbu, et al. and TLS Protocol

Claims 1-11, 13, 14, and 16-27 were rejected under 35 USC §103 (a) as being unpatentable over U.S. Patent No. 6,148,401 of Devanbu, et al. (hereinafter referred to as *Devanbu*) and the Transport Layer Security (TLS) Protocol Version 1.0, RFC 2246 (hereinafter referred to as the *TLS Protocol*).

Claim 1, as amended herein, is as follows:

1. A method comprising:
   requesting a service for a platform from a service provider;
   receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform;
   certifying the use of the service generating a service key pair that is limited to the one or more acceptable configurations of the platform and returning a public key of the key pair to the service provider;
   for the one or more acceptable configurations of the platform; and
   receiving a session key for a session of the service from the service provider, the service being limited to the one or more acceptable configurations of the platform.

Thus, claim 1 provides for requesting a service for a platform from a service provider, and receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform. Claim 1 then provides for generating a service key pair that is limited to the one or more acceptable configurations of the platform and returns a public key of the key pair to the service provider. The claim then provides for certifying the use of the service for one or more acceptable configurations of the platform. Further, the claim provided for receiving a session key for a session of the service from the service provider, where the service is limited to the one or more acceptable configurations of the platform.

It is respectfully submitted that the cited references do not teach or reasonably suggest these claim limitations. While it is submitted that the arguments provided in the previous response remain valid, this response focuses on the amended elements of the claim.

Devanbu relates to a system for providing assurance that a piece of software possesses a particular property. It is again submitted that the reference has no relevance to the certification of a configuration of the platform, but rather is limited to the nature of the software that is being certified. However, regardless of this issue, the reference does not provide for receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform; generating a service key pair that is limited to the one or more acceptable configurations of the platform; or certifying the use of the service for the one or more acceptable configurations of the platform.

As has been previously discussed in the prior response, *Devanbu* describes a determination whether a set of instructions possess a particular property. For example, the summary of *Devanbu* indicate that "a system and method provide assurance to a host that a set of subject instructions adapted to be executed on a host processor possess a property." (*Devanbu*, col. 4, lines 27-30) This is indicating that the set of subject instructions (the software in question) possesses a certain property, without any regard to whether platform has any particular configuration. As the process is described:

> In one embodiment, a verification processor executes a version of a set of verification instructions to determine if the set of subject instructions possess the property. If the set of subject instructions possess the property, then the verification processor cryptographically signs the set of instructions to produce signature information, and in one embodiment of the present invention, distributes the set of instructions with the signature information. In one embodiment, information pertaining to the property verified by the provider can be derived by a host from the set of subject instructions and the signature data. In another embodiment, the provider cryptographically signs property data identifying the property of the set of subject instructions verified by the provider.

(*Devanbu*, col. 4, lines 31-43) In the described process, a verification processor will execute verification instructions to determine if the set of subject instructions possesses a particular property. If this is true, then the verification processor will provide a cryptographic signature for the instructions. The summary further describes how the signature to verify the presence of the property in the subject instructions is used to evaluate the integrity and authenticity of the instructions:

> When a host receives the set of subject instructions and the signature, the host can use the signature to determine the integrity and the authenticity of the subject set of instructions, as well as the identity of the property verified by the provider. If the host cannot certify the set of subject instructions and the property data using the signature information, then the host does not execute the software. If the host can certify the set of subject instructions and the property data, then the host may execute the software.

(*Devanbu*, col. 4, lines 44-52) Thus, if the host can verify the instructions and the property based on the signature, the instructions are executed, and will not execute the instructions otherwise. However, this provides verification of authenticity of software, and is not relevant to a limitation on platform configurations that may utilize a service. In particular, the reference does not provide any suggestion of receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform. No such request is mentioned in the reference. Further, there is no suggestion of the generation of a service key pair that is limited to the one or more acceptable configurations of the platform. The reference does not provide for the generation of any service key that is limited in this manner. Further, there is no suggestion of certifying the use of the service for the one or more acceptable configurations of the platform. The certification described in *Devanbu* regards the authenticity of the software, not a certification of the use of a service for any acceptable platforms.

The *TLS Protocol* then is intended to provide privacy and data integrity between two communicating applications. (See, *TLS Protocol*, Introduction, p. 3) To accomplish this goal, the *TLS Protocol* includes a record protocol and a handshake protocol, with the

record protocol being used to encapsulate higher level protocols and the handshake protocol being used to allow a server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before an application protocol transmits or receives any data. (*TLS Protocol*, Introduction, p. 4) While this provides general security processes, this does not teach or suggest the claim elements that have been shown above to be missing from *Devanbu*. There is no provision in the *TLS Protocol* that relates to receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform; generating a service key pair that is limited to the one or more acceptable configurations of the platform; or certifying the use of the service for the one or more acceptable configurations of the platform..

It is submitted that the arguments presented above are also applicable to the other independent claims provided in the present application, claims 8, 13, 16, 23, and 26. Thus, claims 8, 13, 16, 23, and 26 are also allowable. The remaining rejected claims, while having other differences with the cited references, are allowable as being dependent on the allowable base claims.

Claim Rejection under 35 U.S.C. §103

Devanbu, et al., TLS Protocol, and Klayh, et al.

Claims 12, 15 and 28 were rejected under 35 USC §103 (a) as being unpatentable over *Devanbu* and the *TLS Protocol*, as applied to claims 8, 13, and 27, and further in view of International Patent Publication WO/2000/038089 of Klayh, et al. (hereinafter referred to as *Klayh*).

The rejected claims, while having other differences with the cited references, are allowable as being dependent on the allowable base claims.

Devanbu and the *TLS Protocol* have been addressed above. It is further submitted that the *Klayh* reference, while cited for other purposes, does not contain the claim limitations that, as shown above, are not taught or suggested by *Devanbu* and the *TLS Protocol*. *Klayh* describes an amusement and premiums network, involving a system for controlling a medium of distribution and redemption of loyalty points and coupons. *Klayh* is not relevant to receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform; generating a service key pair that is limited to the one or more acceptable configurations of the platform; or certifying the use of the service for the one or more acceptable configurations of the platform.

Conclusion

Applicant respectfully submits that the rejections have been overcome by the amendment and remark, and that the claims as amended are now in condition for allowance. Accordingly, Applicant respectfully requests the rejections be withdrawn and the claims as amended be allowed.

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (503) 439-8778 if there remains any issue with allowance of the case.

Request for an Extension of Time if Needed

The Applicant respectfully petitions for extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be needed. Please change the fee under 37 C.F.R. § 1.17 for such extension to our Deposit Account No. 02-2666.

Charge our Deposit Account

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 10/15/2007 /Mark C. Van Ness/

Mark C. Van Ness
Reg. No. 39,865

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778